

VIRTUAL PRIVATE LINE NETWORK CONNECTION CONTROL METHOD, VIRTUAL PRIVATE LINE NETWORK CONNECTION CONTROLLER AND VIRUTAL PRIVATE LINE NETWORK CONNECTION SYSTEM

Publication number: JP2002077261

Publication date: 2002-03-15

Inventor: MATSUMOTO MASAOKI; IBUKI MOTOSHI; OKUMURA SATOSHI; SATO KATSUHIKO

Applicant: NIPPON TELEGRAPH & TELEPHONE

Classification:

- international: H04M3/42; H04L12/56; H04M11/00; H04M3/42;
H04L12/56; H04M11/00; (IPC1-7): H04L12/56;
H04M3/42; H04M11/00

- european:

Application number: JP20000264551 20000831

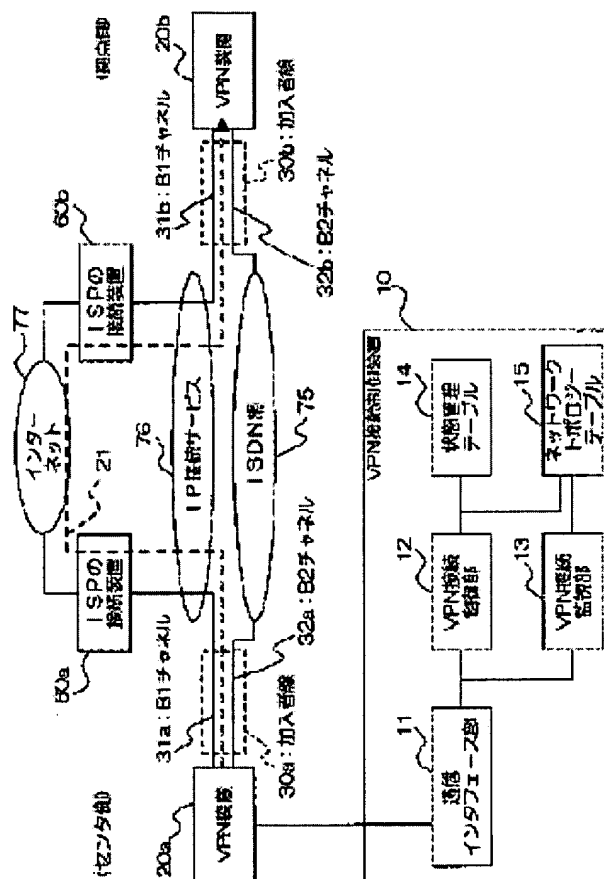
Priority number(s): JP20000264551 20000831

Report a data error here

Abstract of JP2002077261

PROBLEM TO BE SOLVED: To provide a virtual private line network connection control method, its controller and system for connecting VPN devices which even in a communication environment where an IP address is dynamically allocated such as internet connection by means of dial-up.

SOLUTION: The instruction of connection to the Internet is given to the VPN device 20b of a stronghold-side from a VPN connection control part 12, installed in a VPN connection controller 10 via the VPN device 20a and a B2 channel 32a on a center-side and an ISDN network 75. The VPN device 20b receives the instruction and connects it to the connection device 60b of ISP, by using a B1 channel 31b and receives the allocation of the IP address from ISP. The IP address is notified to the VPN connection control part 12 and is written into a state managing table 14. Then, the IP address of the VPN device of a calling destination side is transmitted to the VPN device of a calling source side by communication by using the B2 channel.



(51) Int.Cl. ⁷	識別記号	F I	ターマコード [*] (参考)
H 0 4 L 12/56		H 0 4 M 3/42	Λ 5 K 0 2 4
H 0 4 M 3/42		11/00	3 0 2 5 K 0 3 0
11/00	3 0 2	H 0 4 L 11/20	1 0 2 Λ 5 K 1 0 1

審査請求 未請求 請求項の数10 O L (全 11 頁)

(21) 出願番号 特願2000-264551 (P2000-264551)

(22) 出願日 平成12年8月31日 (2000.8.31)

(71) 出願人 399041158

西日本電信電話株式会社

大阪府大阪市中央区馬場町3番15号

(72) 発明者 松本 政昭

大阪府大阪市中央区馬場町3番15号 西日本電信電話株式会社内

(72) 発明者 伊吹 元志

大阪府大阪市中央区馬場町3番15号 西日本電信電話株式会社内

(74) 代理人 100064908

弁理士 志賀 正武

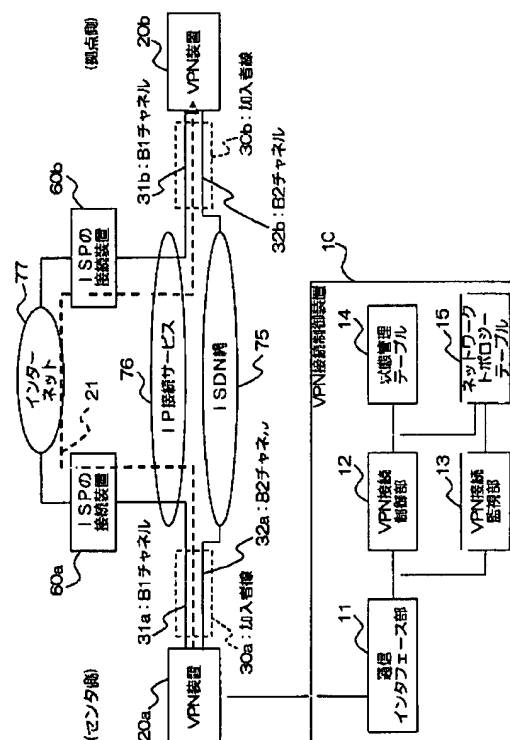
最終頁に続く

(54) 【発明の名称】 仮想専用線網接続制御方法および仮想専用線網接続制御装置ならびに仮想専用線網接続システム

(57) 【要約】

【課題】 ダイヤルアップによるインターネット接続など、IPアドレスが動的に割り振られる通信環境においても、VPN装置同士の接続を可能とする仮想専用線網接続制御方法およびその装置、システムを提供する。

【解決手段】 VPN接続制御装置10に設けられたVPN接続制御部12からセンタ側のVPN装置20aおよびB2チャネル32a、ISDN網75を経由して拠点側のVPN装置20bにインターネットへの接続を指示する。この指示を受けて、VPN装置20bはB1チャネル31bを用いてISPの接続装置60bに接続するとともに、ISPからIPアドレスの割り当てを受ける。このIPアドレスは、VPN接続制御部12に通知され、状態管理テーブル14に書き込まれる。それとともに、B2チャネルを用いた通信によって、発呼先側のVPN装置のIPアドレスが発呼元側のVPN装置に伝えられる。



【特許請求の範囲】

【請求項1】 複数の仮想専用線網装置によって構成される仮想専用線網接続システムの接続を制御する仮想専用線網接続制御装置であって、

前記仮想専用線網装置に動的に割り振られる通信アドレスを保持する管理テーブルと、

各々の前記仮想専用線網装置に動的に割り振られた通信アドレスを受け取って前記管理テーブルに書き込み、発呼先の前記仮想専用線網装置の通信アドレスを前記管理テーブルから読み出して発呼元の前記仮想専用線網装置に通知することによって接続を制御する仮想専用線網接続制御部と、

を備えることを特徴とする仮想専用線網接続制御装置。

【請求項2】 前記仮想専用線網装置は、電話加入者線上の複数の通信チャネルを使用した通信を行い、そのうちの第1の通信チャネルをパブリックなデータ通信網に接続することによってアプリケーションデータを伝送するために使用し、他の第2の通信チャネルを前記通信アドレスの通知を含む接続制御のために使用するものであり、

前記管理テーブルは、前記仮想専用線網装置の前記第2の通信チャネルを用いた通信のための電話番号を保持するものであり、

前記仮想専用線網接続制御部は、前記第1の通信チャネルを前記パブリックなデータ通信網に接続する旨の指示を発呼先の前記仮想専用線網装置に通知するために当該発呼先の前記仮想専用線網装置の前記電話番号を前記管理テーブルから読み出してセンタ側の前記仮想専用線網装置に渡し、センタ側の前記仮想専用線網装置から当該発呼先の前記仮想専用線網装置に動的に割り振られた通信アドレスを受け取って前記管理テーブルに書き込み、発呼元の前記仮想専用線網装置に発呼先の前記仮想専用線網装置の通信アドレスを通知するために前記管理テーブルから発呼先の前記仮想専用線網装置の通信アドレスと発呼元の前記仮想専用線網装置の前記電話番号とを読み出してセンタ側の前記仮想専用線網装置に渡すことによって接続を制御することを特徴とする請求項1に記載の仮想専用線網接続制御装置。

【請求項3】 接続が確立された前記仮想専用線網装置の接続状態を監視する仮想専用線網接続監視部を備え、前記仮想専用線網接続制御部は、前記仮想専用線網接続監視部によって切断が検知された仮想専用線網装置がある場合には、この切断された仮想専用線網装置に関して再度接続を制御する手順を実行することを特徴とする請求項1または2に記載の仮想専用線網接続制御装置。

【請求項4】 仮想専用線網接続における呼の発呼元および発呼先の前記仮想専用線網装置の関係を保持するネットワークポロジータブルを備え、前記仮想専用線網接続制御部は、前記ネットワークポロジータブルのデータに含まれる発呼先の前記仮想専

用線網装置のみに関して接続を制御する手順を実行することを特徴とする請求項1から3までのいずれかに記載の仮想専用線網接続制御装置。

【請求項5】 パブリックなデータ通信網における相手側の通信アドレスを指定することによってアプリケーションデータを相互に伝送しあう複数の仮想専用線網装置によって構成される仮想専用線網接続システムであって、

電話加入者線の第1の通信チャネルを用いて前記パブリックなデータ通信網に接続し、このパブリックなデータ通信網上で仮想専用線網の呼を設定し前記アプリケーションデータを伝送するとともに、電話加入者線の第2の通信チャネルを用いて前記通信アドレスの通知を含む接続制御のための通信を行う複数の仮想専用線網装置と、前記仮想専用線網装置に動的に割り振られる前記パブリックなデータ通信網の通信アドレスと前記仮想専用線網装置の前記第2の通信チャネルを用いた通信のための電話番号を保持する管理テーブルを備え、前記第1の通信チャネルを用いて前記パブリックなデータ通信網に接続する旨の指示を発呼先の前記仮想専用線網装置に通知するために当該発呼先の前記仮想専用線網装置の前記電話番号を前記管理テーブルから読み出してセンタ側の前記仮想専用線網装置に渡し、センタ側の前記仮想専用線網装置から当該発呼先の前記仮想専用線網装置に動的に割り振られた前記通信アドレスを受け取って前記管理テーブルに書き込み、発呼元の前記仮想専用線網装置に発呼先の前記仮想専用線網装置の通信アドレスを通知するために前記管理テーブルから発呼元の前記仮想専用線網装置の通信アドレスと発呼元の前記仮想専用線網装置の前記電話番号とを読み出してセンタ側の前記仮想専用線網装置に渡すことによって接続を制御する仮想専用線網接続制御装置と、

によって構成され、

センタ側の前記仮想専用線網装置は前記第1の通信チャネルを用いて前記パブリックなデータ通信網に接続する旨の指示を、前記仮想専用線網接続制御装置から発呼元の前記仮想専用線網装置に通知するために発呼元の前記仮想専用線網装置の前記電話番号を受け取った際には前記第2の通信チャネルを用いて当該電話番号に対する通信を設定してこの指示を通知し、当該発呼元の前記仮想専用線網装置に動的に割り振られた通信アドレスをこの仮想専用線網装置から受け取った際にはこの通信アドレスを前記仮想専用線網接続制御装置に渡し、前記仮想専用線網接続制御装置から発呼元の前記仮想専用線網装置に発呼元の前記仮想専用線網装置の通信アドレスを通知するために前記管理テーブルから発呼元の前記仮想専用線網装置の通信アドレスと発呼元の前記仮想専用線網装置の前記電話番号とを受け取った際には前記第2の通信チャネルを用いて当該電話番号に対する通信を設定して当該発呼元の前記仮想専用線網装置の通信アドレスを通

知することを特徴とする仮想専用線網接続システム。

【請求項6】 前記仮想専用線網接続制御装置は、接続が確立された前記仮想専用線網装置の接続状態を監視し、接続が切断された前記仮想専用線網装置を検知した場合には、この切断された仮想専用線網装置に関して再度接続を制御する手順を実行することを特徴とする請求項5に記載の仮想専用線網接続システム。

【請求項7】 前記仮想専用線網接続制御装置は、仮想専用線網接続における呼の発呼元および発呼先の前記仮想専用線網装置の関係を保持するネットワークポロジータブルを備え、前記ネットワークポロジータブルのデータに含まれる発呼先の前記仮想専用線網装置のみに関して接続を制御する手順を実行することを特徴とする請求項5または6に記載の仮想専用線網接続システム。

【請求項8】 第1の通信チャネルおよび第2の通信チャネルを使用可能でありパブリックなデータ通信網上で相手側の通信アドレスを指定することによってアプリケーションデータを相互に伝送しあう複数の仮想専用線網装置と、これらの仮想専用線網装置間の接続を制御する仮想専用線網接続制御装置とによって構成される仮想専用線網接続システムにおける仮想専用線網接続制御方法であって、

仮想専用線網接続制御装置が自己の保有する管理テーブルから発呼先の前記仮想専用線網装置の電話番号を読み出して該電話番号をセンタ側の前記仮想専用線網装置に渡し、この電話番号を受け取ったセンタ側の前記仮想専用線網装置が前記第2の通信チャネルを使用してこの電話番号に対する通信を設定する第1の過程と、

センタ側の前記仮想専用線網装置が、前記第2の通信チャネルを通して、発呼先の前記仮想専用線網装置に対して、前記パブリックなデータ通信網に接続する旨の指示を行う第2の過程と、

この指示を受けた発呼側の前記仮想専用線網装置が、前記第1の通信チャネルを用いて前記パブリックなデータ通信網に接続する第3の過程と、

当該発呼側の仮想専用線網装置に動的に割り振られた前記パブリックなデータ通信網における通信アドレスを、当該発呼側の仮想専用線網装置からセンタ側の前記仮想専用線網装置を経由して前記仮想専用線網接続制御装置に通知し、これを受けた前記仮想専用線網接続制御装置が前記管理テーブルにこの通信アドレスを書き込む第4の過程と、

前記仮想専用線網接続制御装置が前記管理テーブルから発呼元の前記仮想専用線網装置の電話番号と発呼先の前記仮想専用線網装置の前記通信アドレスとを読み出してセンタ側の前記仮想専用線網装置に渡し、これを受けたセンタ側の前記仮想専用線網装置が前記第2の通信チャネルを用いて当該電話番号に対する呼を設定して当該発呼元の仮想専用線網装置に対して当該発呼先の仮想専用

線網装置の通信アドレスを通知する第5の過程と、

この通知を受けた発呼元の前記仮想専用線網装置が当該通信アドレスを用いて前記パブリックなデータ通信網上で発呼先の前記仮想専用線網装置との間の呼を設定する第6の過程と、

を有することを特徴とする仮想専用線網接続制御方法。

【請求項9】 前記仮想専用線網接続制御装置が、接続が確立された前記仮想専用線網装置の接続状態を監視する接続監視過程と、

前記接続監視過程において切断が検知された仮想専用線網装置がある場合には、前記仮想専用線網接続制御装置がこの切断された仮想専用線網装置に関して再度接続を制御する再接続過程と、を有することを特徴とする請求項8に記載の仮想専用線網接続制御方法。

【請求項10】 仮想専用線網接続における呼の発呼元および発呼先の前記仮想専用線網装置の関係を保持するネットワークポロジータブルのデータに含まれる発呼先の前記仮想専用線網装置のみに関して前記第1から第6までの過程の手順を実行することを特徴とする請求項8または9に記載の仮想専用線網接続制御方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、主としてインターネットを用いて、仮想的な専用線網を構築するための複数の仮想専用線網装置間の接続を制御する仮想専用線網接続制御装置およびその方法に関する。

【0002】

【従来の技術】従来の技術において、仮想専用線網（以下では、VPN (Virtual Private Network) と略称する）は以下のように構築されていた。複数の拠点にそれぞれVPN装置を設置し、各VPN装置の通信アドレスを予め管理情報として保持しておく。また、各々のVPN装置は近くのアクセスポイントを通してインターネットに接続可能としておく。そして、予め定義されたネットワークポロジータブルに従って、発呼元のVPN装置が発呼先の通信アドレスを指定してインターネット経由での接続を確立することにより、このVPNを介した通信が可能となる。なお、上記のVPN装置間の通信はIP (インターネットプロトコル) によって行われ、通信アドレスとしてはIPアドレスが用いられる。

【0003】

【発明が解決しようとする課題】公衆網を利用してISP (インターネットサービスプロバイダ) に対してダイヤルアップ接続を行うような通信環境においては、予め固定的なIPアドレスが割り振られているのではなく、ダイヤルアップ接続時に、例えばDHCP (Dynamic Host Configuration Protocol) などを用いて動的にIPアドレスが割り振られるようになっていることが多い。このような動的なアドレス割当ては、限りあるIPアドレス (グローバルIPアドレス) の空間を有効に活用す

ること、および、ISP側のアドレス管理のための手間とコストを軽減することなどを目的としている。

【0004】しかしながら、上記従来技術では、各VPN装置のIPアドレスを予め保持しておくことが前提となっているため、固定的なIPアドレスをVPN装置に割当てることができる通信環境でしかVPNを構築できないという問題があった。そこで、IPアドレスが予め固定されてないダイヤルアップ接続などの通信環境においても、利用可能なVPN装置が求められている。

【0005】本発明は、上記のような事情を考慮してなされて物であり、ダイヤルアップによるインターネット接続など、IPアドレスが動的に割り振られる通信環境においても、VPN装置同士の接続を可能とする仮想専用線網接続制御方法および仮想専用線網接続制御装置ならびに仮想専用線網接続システムを提供することを目的とする。

【0006】

【課題を解決するための手段】上記の課題を解決するために、この発明による仮想専用線網接続制御装置は、複数の仮想専用線網装置によって構成される仮想専用線網接続システムの接続を制御する仮想専用線網接続制御装置であって、前記仮想専用線網装置に動的に割り振られる通信アドレスを保持する管理テーブルと、各々の前記仮想専用線網装置に動的に割り振られた通信アドレスを受け取って前記管理テーブルに書き込み、発呼先の前記仮想専用線網装置の通信アドレスを前記管理テーブルから読み出して発呼元の前記仮想専用線網装置に通知することによって接続を制御する仮想専用線網接続制御部とを備えることを特徴とする。

【0007】また、この発明による仮想専用線網接続制御装置においては、前記仮想専用線網装置は、電話加入者線上の複数の通信チャネルを使用した通信を行い、そのうちの第1の通信チャネルをパブリックなデータ通信網に接続することによってアプリケーションデータを伝送するために使用し、他の第2の通信チャネルを前記通信アドレスの通知を含む接続制御のために使用するものであり、前記管理テーブルは、前記仮想専用線網装置の前記第2の通信チャネルを用いた通信のための電話番号を保持するものであり、前記仮想専用線網接続制御部は、前記第1の通信チャネルを前記パブリックなデータ通信網に接続する旨の指示を発呼先の前記仮想専用線網装置に通知するために当該発呼先の前記仮想専用線網装置の前記電話番号を前記管理テーブルから読み出してセンタ側の前記仮想専用線網装置に渡し、センタ側の前記仮想専用線網装置から当該発呼先の前記仮想専用線網装置に動的に割り振られた通信アドレスを受け取って前記管理テーブルに書き込み、発呼元の前記仮想専用線網装置に発呼先の前記仮想専用線網装置の通信アドレスを通知するために前記管理テーブルから発呼元の前記仮想専用線網装置の通信アドレスと発呼元の前記仮想専用線網

装置の前記電話番号とを読み出してセンタ側の前記仮想専用線網装置に渡すことによって接続を制御することを特徴とする。ここで、電話加入者線上の複数の通信チャネルとは、例えばISDN (Integrated Services Digital Networks, 統合デジタルサービス網) における複数のチャネルである。例えば、加入者線毎に2本のBチャネルと1本のDチャネルが収容される「2B+D」の構成である場合、2本のうちの1本のBチャネルを前記第1の通信チャネルとして使用し、他の1本のBチャネルを前記第2の通信チャネルとして使用することができる。また、使用可能な通信チャネルの数がより多い場合、例えば23本のBチャネルと1本のDチャネルとで構成される「23B+D」の構成の場合には、第1の通信チャネルとして複数のBチャネルを割当てても良いし、第2の通信チャネルとして複数のBチャネルを割当てても良い。また、ここで、パブリックなデータ通信網の代表例はインターネットである。このようなパブリックなデータ通信網は比較的低コストで利用できるため、これを用いて仮想的な専用線網を構築する場合、実際に専用回線をリースする場合に比べて安価な実現が可能となる。

【0008】また、この発明による仮想専用線網接続制御装置においては、接続が確立された前記仮想専用線網装置の接続状態を監視する仮想専用線網接続監視部を備え、前記仮想専用線網接続制御部は、前記仮想専用線網接続監視部によって切断が検知された仮想専用線網装置がある場合には、この切断された仮想専用線網装置に関して再度接続を制御する手順を実行することを特徴とする。

【0009】また、この発明による仮想専用線網接続制御装置においては、仮想専用線網接続における呼の発呼元および発呼先の前記仮想専用線網装置の関係を保持するネットワークポロジータブルを備え、前記仮想専用線網接続制御部は、前記ネットワークポロジータブルのデータに含まれる発呼先の前記仮想専用線網装置のみに関して接続を制御する手順を実行することを特徴とする。

【0010】また、この発明による仮想専用線網接続システムは、パブリックなデータ通信網における相手側の通信アドレスを指定することによってアプリケーションデータを相互に伝送しあう複数の仮想専用線網装置によって構成される仮想専用線網接続システムであって、電話加入者線の第1の通信チャネルを用いて前記パブリックなデータ通信網に接続し、このパブリックなデータ通信網上で仮想専用線網の呼を設定し前記アプリケーションデータを伝送するとともに、電話加入者線の第2の通信チャネルを用いて前記通信アドレスの通知を含む接続制御のための通信を行う複数の仮想専用線網装置と、前記仮想専用線網装置に動的に割り振られる前記パブリックなデータ通信網の通信アドレスと前記仮想専用線網装

置の前記第2の通信チャネルを用いた通信のための電話番号を保持する管理テーブルを備え、前記第1の通信チャネルを用いて前記パブリックなデータ通信網に接続する旨の指示を発呼先の前記仮想専用線網装置に通知するために当該発呼先の前記仮想専用線網装置の前記電話番号を前記管理テーブルから読み出してセンタ側の前記仮想専用線網装置に渡し、センタ側の前記仮想専用線網装置から当該発呼先の前記仮想専用線網装置に動的に割り振られた前記通信アドレスを受け取って前記管理テーブルに書き込み、発呼元の前記仮想専用線網装置に発呼先の前記仮想専用線網装置の通信アドレスを通知するために前記管理テーブルから発呼先の前記仮想専用線網装置の通信アドレスと発呼元の前記仮想専用線網装置の前記電話番号とを読み出してセンタ側の前記仮想専用線網装置に渡すことによって接続を制御する仮想専用線網接続制御装置とによって構成され、センタ側の前記仮想専用線網装置は前記第1の通信チャネルを用いて前記パブリックなデータ通信網に接続する旨の指示を、前記仮想専用線網接続制御装置から発呼先の前記仮想専用線網装置に通知するために発呼先の前記仮想専用線網装置の前記電話番号を受け取った際には前記第2の通信チャネルを用いて当該電話番号に対する通信を設定してこの指示を通知し、当該発呼先の前記仮想専用線網装置に動的に割り振られた通信アドレスをこの仮想専用線網装置から受け取った際にはこの通信アドレスを前記仮想専用線網接続制御装置に渡し、前記仮想専用線網接続制御装置から発呼元の前記仮想専用線網装置に発呼先の前記仮想専用線網装置の通信アドレスを通知するために前記管理テーブルから発呼先の前記仮想専用線網装置の通信アドレスと発呼元の前記仮想専用線網装置の前記電話番号とを受け取った際には前記第2の通信チャネルを用いて当該電話番号に対する通信を設定して当該発呼先の前記仮想専用線網装置の通信アドレスを通知することを特徴とする。

【0011】また、この発明による仮想専用線網接続システムにおいては、前記仮想専用線網接続制御装置は、接続が確立された前記仮想専用線網装置の接続状態を監視し、接続が切断された前記仮想専用線網装置を検知した場合には、この切断された仮想専用線網装置に関して再度接続を制御する手順を実行することを特徴とする。

【0012】また、この発明による仮想専用線網接続システムにおいては、前記仮想専用線網接続制御装置は、仮想専用線網接続における呼の発呼元および発呼先の前記仮想専用線網装置の関係を保持するネットワークポロジータブルを備え、前記ネットワークポロジータブルのデータに含まれる発呼先の前記仮想専用線網装置のみに関して接続を制御する手順を実行することを特徴とする。

【0013】また、この発明による仮想専用線網接続制御方法は、第1の通信チャネルおよび第2の通信チャネ

ルを使用可能でありパブリックなデータ通信網上で相手側の通信アドレスを指定することによってアプリケーションデータを相互に伝送しあう複数の仮想専用線網装置と、これらの仮想専用線網装置間の接続を制御する仮想専用線網接続制御装置とによって構成される仮想専用線網接続システムにおける仮想専用線網接続制御方法であって、仮想専用線網接続制御装置が自己の保有する管理テーブルから発呼先の前記仮想専用線網装置の電話番号を読み出して該電話番号をセンタ側の前記仮想専用線網装置に渡し、この電話番号を受け取ったセンタ側の前記仮想専用線網装置が前記第2の通信チャネルを使用してこの電話番号に対する通信を設定する第1の過程と、センタ側の前記仮想専用線網装置が、前記第2の通信チャネルを通して、発呼先の前記仮想専用線網装置に対して、前記パブリックなデータ通信網に接続する旨の指示を行う第2の過程と、この指示を受けた発呼側の前記仮想専用線網装置が、前記第1の通信チャネルを用いて前記パブリックなデータ通信網に接続する第3の過程と、当該発呼側の仮想専用線網装置に動的に割り振られた前記パブリックなデータ通信網における通信アドレスを、当該発呼側の仮想専用線網装置からセンタ側の前記仮想専用線網装置を経由して前記仮想専用線網接続制御装置に通知し、これを受けた前記仮想専用線網接続制御装置が前記管理テーブルにこの通信アドレスを書き込む第4の過程と、前記仮想専用線網接続制御装置が前記管理テーブルから発呼元の前記仮想専用線網装置の電話番号と発呼先の前記仮想専用線網装置の前記通信アドレスとを読み出してセンタ側の前記仮想専用線網装置に渡し、これを受けたセンタ側の前記仮想専用線網装置が前記第2の通信チャネルを用いて当該電話番号に対する呼を設定して当該発呼元の仮想専用線網装置に対して当該発呼先の仮想専用線網装置の通信アドレスを通知する第5の過程と、この通知を受けた発呼元の前記仮想専用線網装置が当該通信アドレスを用いて前記パブリックなデータ通信網上で発呼先の前記仮想専用線網装置との間の呼を設定する第6の過程とを有することを特徴とする。

【0014】また、この発明による仮想専用線網接続制御方法においては、前記仮想専用線網接続制御装置が接続が確立された前記仮想専用線網装置の接続状態を監視する接続監視過程と、前記接続監視過程において切断が検知された仮想専用線網装置がある場合には前記仮想専用線網接続制御装置がこの切断された仮想専用線網装置に関して再度接続を制御する再接続過程とを有することを特徴とする。

【0015】また、この発明による仮想専用線網接続制御方法は、仮想専用線網接続における呼の発呼元および発呼先の前記仮想専用線網装置の関係を保持するネットワークポロジータブルのデータに含まれる発呼先の前記仮想専用線網装置のみに関して前記第1から第6までの過程の手順を実行することを特徴とする。

【0016】

【発明の実施の形態】以下、図面を参照しこの発明の一実施形態について説明する。本実施形態では、IPアドレスが固定されていないダイヤルアップ接続環境でVPN接続するため、複数のVPN装置のうちの1台をセンタ側VPN装置と位置付け、そのセンタ側VPN装置に、各VPN装置の電話番号、IPアドレス、接続/切断のフラグを管理するテーブルを備えたVPN接続制御装置を併設することとする。例えば、VPN接続を構築する企業においては、センタ側VPN装置を本店に設置し、その他の拠点側VPN装置を支店や営業所等に設置する。

【0017】この構成によりVPN接続する場合の手順は、次の通りである。(1) ISDN回線のB2チャネルを利用して、センタ側VPN装置から拠点側VPN装置に対して接続要求を行う。(2) これを受けた拠点側VPN装置は、ダイヤルアップによってISPの接続装置に対して接続要求を行い、ISPの接続装置から通知されたIPアドレスを、センタ側VPN装置を介してVPN接続制御装置に通知する。(3) VPN接続制御装置は、各拠点側VPN装置から通知されたIPアドレスをテーブルに記録する。(4) VPN接続制御装置は、各VPN装置に対し、それぞれのVPN装置の接続先となるVPN装置のIPアドレスを送信し、これを受信したVPN装置はVPN接続制御装置からそのIPアドレスに対する接続を行い、VPN接続を確立する。(5) 接続完了後、VPN接続制御装置は各VPN装置の接続状態を監視し、何らかの原因で接続が切断された場合には、そのVPN装置に対し前記(1)から(4)に示した接続手順を実行し、接続の再構築を行う。

【0018】図1は、本実施形態によるVPN接続システム(仮想専用線網接続システム)の構成を示す構成図である。図1において、符号20aおよび20bはそれぞれセンタ側および拠点側のVPN装置(仮想専用線網装置)、30aおよび30bはそれぞれVPN装置20aおよび20bに接続されたISDNの加入者線である。加入者線30aには、時分割多重化方式により複数のチャネルが論理的に収容されており、その中にはB1チャネル31a(第1の通信チャネル)およびB2チャネル32a(第2の通信チャネル)が含まれている。また、加入者線30bには同様にB1チャネル31bおよびB2チャネル32bが含まれている。また、75はISDN網、76は加入者線を利用してISP等への接続を行うためのIP接続サービス、77はインターネット(パブリックなデータ通信網)である。また、60aおよび60bは、それぞれセンタ側および拠点側から接続するためのISPの接続装置である。

【0019】図1に示す構成においては、センタ側のVPN装置20aはB1チャネル31aを使用してISPの接続装置60aに接続でき、拠点側のVPN装置20

bはB1チャネル31bを使用してISPの接続装置60bに接続できるようになっている。これにより、インターネット77を経由する経路21によって、VPN装置20aと20bとの間での通信が可能となる。また、それぞれのVPN接続装置は、B2チャネル32aおよび32bを用いてISDN網75を経由して相互に通信を行うことが可能である。

【0020】また、10は、センタ側VPN装置20aに接続されておりVPN装置間の接続を制御するためのVPN接続制御装置(仮想専用線網接続制御装置)であり、このVPN接続制御装置10は、内部に通信インタフェース部11とVPN接続制御部12とVPN接続監視部13と状態管理テーブル14(管理テーブル)とネットワークトポロジーテーブル15とを有している。

【0021】図2は、状態管理テーブル14のデータ構造およびデータ例を示す表図である。図2に示すように、状態管理テーブル14は、VPN装置名、ISDN番号、グローバルIPアドレス、状態をデータ項目として持つ表形式のデータである。これらのデータ項目のうち、グローバルIPアドレスは、各VPN装置に割り振られたIPアドレスがVPN接続制御装置に通知されたときに書き込まれる。また、状態は、各VPN装置から接続/切断が通知されたときやVPN接続監視部13によって状態変化が検出されたときに書き換えられる。図2に示すデータ例では、A～Eの5つのVPN装置を管理する情報が状態管理テーブルによって保持されている。なお、本例では、Aがセンタ側のVPN装置であり、B～Eの4つが拠点側のVPN装置である。

【0022】次に、VPN接続制御装置10の制御によって、各VPN装置が自己以外のすべてのVPN装置に対して接続を行うための手順を説明する。図5は、その手順を示すフローチャートである。

【0023】(ステップS11) 図5の手順において、まず、VPN接続制御装置10のVPN接続制御部12が状態管理テーブル14を参照する。そして、VPN制御装置10からセンタ側(サーバ側)のVPN装置に対する指示により、センタ側のVPN装置Aは、状態が「接続」ではないすべてのVPN装置に対して(図2に示すデータ例においては、VPN装置DおよびEに対して)、B2チャネルを用いてISDN網経由での呼設定を行う。なお、その際には状態管理テーブル14から得られるISDN番号が用いられる。

(ステップS12) そして、センタ側のVPN装置Aは、接続先のVPN装置に対して、IP接続サービスへのダイヤルアップを行うように依頼する。

【0024】(ステップS13) 上記の依頼を受けた拠点側のVPN装置は、B1チャネルを用いたダイヤルアップによってISPの接続装置に接続する。

(ステップS14) そして、拠点側のVPN装置は、接続したISPの接続装置から自己のグローバルIPアド

レスを取得する。このグローバルIPアドレスは、拠点側のVPN装置からB2チャンネルを用いてセンタ側のVPN装置に通知され、さらにVPN接続制御装置10のVPN接続制御制御部に伝えられて状態管理テーブル14に書き込まれる。なお、センタ側のVPN装置自体の状態が「接続」でない場合にも、上記と同様に、B1チャンネルを用いてISPの接続装置への接続が行われ、割り振られたグローバルIPアドレスが状態管理テーブル14に書き込まれる。

【0025】(ステップS15)すべてのVPN装置がインターネットに接続されると、B2チャンネルを用いた通信により、状態管理テーブルに管理されている全VPN装置のグローバルIPアドレスが各々のVPN装置に通知される。

(ステップS16)上記の通知を受けた各VPN装置は、通知を受けたIPアドレスに対してVPNトンネルを設定する。

【0026】(ステップS17)VPN接続監視部13は、所定の時間間隔ですべてのVPN装置に対して監視信号を送出し、接続状態を監視する。そして、その状況に応じて適宜、状態管理テーブル14の状態の項目を更新する。ここで、もしいずれかのVPN接続装置から監視信号に対する応答がなく切断と判断した場合には、ステップS11に戻って再接続の手順を実行する。また、監視信号に対して正常応答が得られた場合には、正常接続状態であると認識するとともに、次の監視信号送出のタイミングまで待つ。正常接続状態においては、ステップS16において設定されたVPNトンネルを通して、VPNのアプリケーションデータがVPN装置間で伝送される。

【0027】図6は、上記接続手順によって、全VPN装置間で相互に接続が設定されたときのネットワークトポロジーを示す参考図である。図6において、A～EはそれぞれVPN監視装置を表わし、それらを結ぶ矢印線はVPN装置間の接続を表わす。なお、矢印線の根元側が発呼元であり、先側が発呼先である。

【0028】上に述べた方法では、例えば営業所－営業所間のように通信トラフィックが無いもしくは非常に少ない対地においてもVPNトンネルを構築し、監視信号を全てのVPN装置に送るため、ネットワーク上に不必要に多くのパケットを送出することになるとともに、営業所等のVPN装置にも高い負荷をかけることになってしまう。そこで、例えば、本社－支店間、本社－営業所間、支店－営業所間など通信の必要がある対地間だけにVPNトンネルを設定する方法を次に説明する。

【0029】図3は、ネットワークトポロジーを定義するためのネットワークトポロジーテーブル15のデータ構造及びデータ例を示す表図である。このネットワークトポロジーテーブルは、発呼元VPN装置名と発呼先VPN装置名の項目を有しており、各VPN装置をノード

とする有向グラフと等価なデータを表形式で保持している。その有向グラフのノードがVPN装置間で確立される接続を表わしている。図3に示すデータ例は、A(発呼元)→B(発呼先)、B→A、C→A、C→B、D→A、D→B、E→A、E→Bの接続によってVPNを構築することを表わしている。

【0030】図7は、ネットワークトポロジーテーブルを参照しながら、必要な対地間のみで接続を行うための手順を示すフローチャートである。

【0031】(ステップS21)図7の手順において、まず、VPN接続制御装置10のVPN接続制御部12がネットワークトポロジーテーブル15を参照する。そして、発呼先VPN装置名となっているVPN装置のISDN番号を状態管理テーブル14から取得する。そして、センタ側(サーバ側)のVPN装置からこれら発呼先のVPN装置に対して、B2チャンネルを用いてダイヤルし、ISDN網の呼を設定する。例えば、図3に示したデータ例の場合、発呼先VPN装置名の項目に含まれているのは「A」および「B」の2つであり、これらのVPN装置のISDN番号は図2に示したデータ例によると、それぞれ「06-4803-1111」および「06-4804-2222」である。なお、ここで、AからBへはB2チャンネルを用いたダイヤルは行われるが、Aはセンタ側VPN装置そのものであるため、AからAへのダイヤルは行う必要はない。

【0032】(ステップS22)次に、センタ側のVPN装置から各発呼先のVPN装置に対して、IP接続サービスへのダイヤルアップを行うように指示が行われる。

(ステップS23)この指示に基づき、各発呼先VPN装置は、B1チャンネルを用いて、ISPの接続装置への接続を行う。なお、図3に示すようにセンタ側VPN装置(A)が発呼先VPN装置に含まれている場合には、センタ側VPN装置からもISP接続装置への接続が行われる。

(ステップS24)そして、ISPの接続装置への接続を行ったVPN装置は、ISPからグローバルIPアドレスを取得し、そのグローバルIPアドレスはセンタ側のVPN装置を経由してVPN接続制御部12に伝えられ、VPN接続制御部12によって状態管理テーブル14に書き込まれる。

【0033】(ステップS25)次に、VPN接続制御部12は、ネットワークトポロジーテーブル15を参照し、発呼元となっているそれぞれのVPN装置に関して、その発呼元VPN装置のISDN番号を状態管理テーブル14から取得するとともに、各発呼元VPN装置に対応する発呼先VPN装置のグローバルIPアドレスを同じく状態管理テーブル14から取得する。そして、センタ側VPN装置は、B2チャンネルを用いて各々の発呼元VPN装置のISDN番号をダイヤルし、その発呼

元VPN装置に対して、対応する発呼先VPN装置のグローバルIPアドレスを通知する。例えば、図2および図3に示すデータ例の場合、ネットワークポロジータブル15には発呼元VPN装置名として「B」が含まれており、この「B」に対応する発呼先VPN装置名は「A」となっている。従って、センタ側VPN装置は、状態管理テーブル14に書かれているBのISDN番号「06-4804-2222」をダイヤルしてVPN装置Bに接続し、AのグローバルIPアドレス「x. x. x. x」を通知する。また、例えば、ネットワークポロジータブル15に発呼元VPN装置名として含まれている「D」に関して、この「D」に対応する発呼先VPN装置名は「A」および「B」であるので、センタ側VPN装置は、VPN装置DのISDN番号「06-4806-4444」をダイヤルしてVPN装置Dに接続し、VPN装置AおよびBのグローバルIPアドレス「x. x. x. x」および「y. y. y. y」を通知する。なお、ここではIPアドレスを「x. x. x. x」および「y. y. y. y」と表わしたが、実際には具体的な数値によって構成されるアドレスが通知される。

【0034】(ステップS26)そして、通知を受けた各々の発呼元VPN装置は、必要に応じてISPの接続装置に接続してから、通知されたIPアドレスに対してVPNトンネルを設定する。

(ステップS27)VPN接続監視部13は、所定の時間間隔ですべての発呼先となっているVPN装置に対して監視信号を送出し、設定状態を監視する。そして、その状況に応じて適宜、状態管理テーブル14の状態の項目を更新する。ここで、もしいずれかのVPN接続装置から監視信号に対する応答がなく切断と判断した場合には、ステップS21に戻って再接続の手順を実行する。また、監視信号に対して正常応答が得られた場合には、正常接続状態にあると認識するとともに、次の監視信号送出のタイミングまで待つ。

【0035】この手順によると、ネットワークポロジータブルに従って、限られたVPN装置間のみVPNトンネルを設定し、発呼先となっているVPN装置のみに監視信号を送出するため、ネットワーク上に不必要に多くのパケットを送出することもなく、営業所等のVPN装置の負荷を軽減することが可能となる。また、これにより、営業所等のVPN装置の性能規模を小さくすることもできるため、システム全体のコストを抑制することが可能となる。

【0036】図8は、上記接続手順によって、ネットワークポロジータブルに定義されたVPN装置間のみで接続が設定されたときのネットワークポロジータブルを示す参考図である。図8に示すように、VPN装置AからはBのみに、同じくBからはAのみに、またC、D、EからはそれぞれAおよびBのみにに対して発呼が行われている。

【0037】次に、予め定められたタイムスケジュールに従ってVPN接続の設定をさらに限定する方法について説明する。なおこの方法は、ネットワークポロジータブルに定義された全ての接続に関して24時間365日フルに呼を設定する必要がない場合に有用である。図4は、VPN装置毎の稼働スケジュールを情報として含む状態管理テーブルのデータ構造およびデータ例を示す表図である。この図に示す状態管理テーブルには、VPN装置名とISDN番号とグローバルIPアドレスと状態のほか、スケジュールがデータ項目として付加された表形式のデータである。図4に示すデータ例では、VPN装置Aは停止することなくフル稼働するスケジュールとなっており、VPN装置Bは土曜日および日曜日に停止、VPN装置C～Eは平日の日勤帯のみ稼働するというスケジュールになっている。そして、VPN接続制御部12は、VPN接続制御装置10に内蔵されているカレンダー機能および時計機能の情報を参照することによって、この状態管理テーブルに定義されたスケジュールに従って、稼働させるべきVPN装置接続させるような制御を行う。つまり、各VPN装置が稼働すべき時間帯においてのみ、そのVPN装置に関する初期起動や接続監視を行う。また、稼働すべき時間帯の終了時点には、VPN接続を切断する手順を行う。

【0038】上述したVPN接続制御装置は、例えば、コンピュータシステムを用いて実現する。具体的には、VPN接続制御部12およびVPN接続監視部13は、図5や図7を用いて説明した手順に応じた処理をプログラムの形式でコンピュータシステムの記憶装置に記憶しておき、中央処理装置がそのプログラムを読み出して実行することによって実現する。また、通信インタフェース部11は、コンピュータシステムの入出力装置およびそれを駆動するプログラムによって実現し、ケーブル等を介してVPN装置20aと信号のやりとりを行うとともに、その信号内容に応じた情報をVPN接続制御部12やVPN接続監視部13との間で授受する。そして、状態管理テーブル14およびネットワークポロジータブル15は、その構造に応じた表現形式のデータをコンピュータシステムの記憶装置に記憶させることによって実現する。ここで、記憶装置とは、例えば、磁気ディスクや半導体メモリなどを用いる。

【0039】

【発明の効果】以上説明したように、この発明によれば、仮想専用線網接続制御装置に仮想専用線網装置に動的に割り振られる通信アドレスを保持する管理テーブルを備え、発呼先仮想専用線網装置の通信アドレスを仮想専用線網接続制御装置から発呼元仮想専用線網装置に通知するため、発呼元側に予め固定的な通信アドレスの情報を設定しておかなくても、発呼元側から発呼先側に呼を設定し、仮想専用線網の接続を実現することができる。従って、例えばIP接続サービスのダイヤルアップ

接続のように通信アドレスが動的に割り振られるような通信環境においても、固定的な通信アドレスが割り振られる常時接続サービスと同等の接続を実現できる。具体的には、例えば、ダイヤルアップによるインターネット接続を利用した仮想専用線網の構築が可能となる。

【0040】また、この発明によれば、接続が確立された後、例えば監視用のパケットを用いるなどして仮想専用線網装置の接続状態を監視し、接続が切断された場合には再接続の手順を実行するため、障害時にも自動的な接続の復旧を試みる耐障害性の高い仮想専用線網を実現することが可能となる。

【0041】また、この発明によれば、仮想専用線網接続制御装置に接続の方向性を考慮したネットワークポロジータブルを備え、このネットワークポロジータブルに仮想専用線網装置の発呼元および発呼先の関係を定義し、この情報に基づいて呼の設定を行うとともに、このテーブルに発呼先と定義された仮想専用線網装置のみについて上記の接続監視を行うため、監視信号を必要最低限に抑え、仮想専用線網装置の負荷を軽減し、不要なパケットトラヒックの排除を行うことによって、より一層実効効率の高いデータ転送を行う仮想専用線網を実現することが可能となる。

【図面の簡単な説明】

【図1】 この発明の一実施形態によるVPN接続システムの構成を示す構成図である。

【図2】 同実施形態によるVPN接続制御装置に設けられた状態管理テーブル（14）のデータ構造およびデータの一例を示す表図である。

【図3】 同実施形態によるVPN接続制御装置に設けられたネットワークポロジータブル（15）のデータ構造およびデータの一例を示す表図である。

【図4】 同実施形態によるVPN接続制御装置に設けられた状態管理テーブル（14）のデータ構造およびデータの他の例を示す表図である。

【図5】 同実施形態によるVPN接続制御の手順を示すフローチャートである。

【図6】 同実施形態により、全VPN装置間で相互に接続が設定されたときのネットワークポロジータブルを示す参考図である。

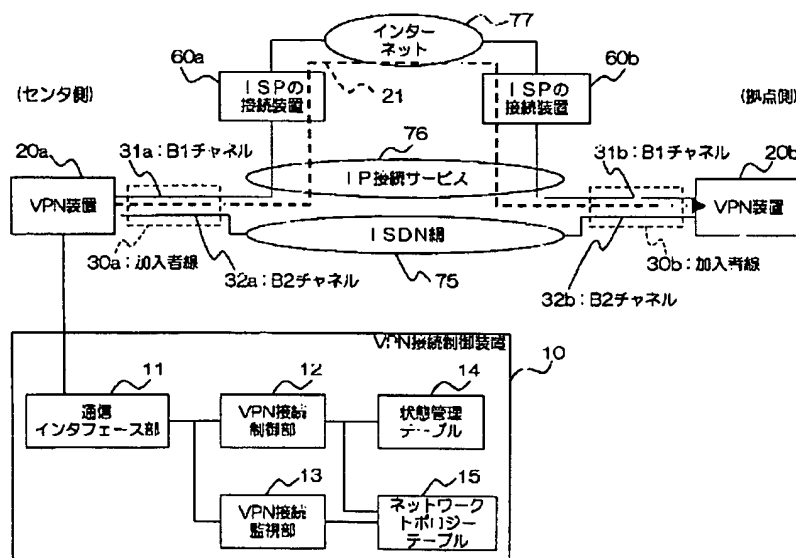
【図7】 同実施形態により、ネットワークポロジータブルを参照しながら、必要な対地間のみで接続を行う手順を示すフローチャートである。

【図8】 同実施形態により、ネットワークポロジータブルに定義されたVPN装置間のみで接続が設定されたときのネットワークポロジータブルの一例を示す参考図である。

【符号の説明】

- 10 VPN接続制御装置
- 11 通信インタフェース部
- 12 VPN接続制御部
- 13 VPN接続監視部
- 14 状態管理テーブル
- 15 ネットワークポロジータブル
- 20a, 20b VPN装置
- 30a, 30b 加入者線
- 31a, 31b B1チャンネル
- 32a, 32b B2チャンネル
- 60a, 60b ISPの接続装置
- 75 ISDN網
- 76 IP接続サービス
- 77 インターネット

【図1】



【図3】

発呼元VPN装置名	発呼先VPN装置名
A	B
B	A
C	A,B
D	A,B
E	A,B

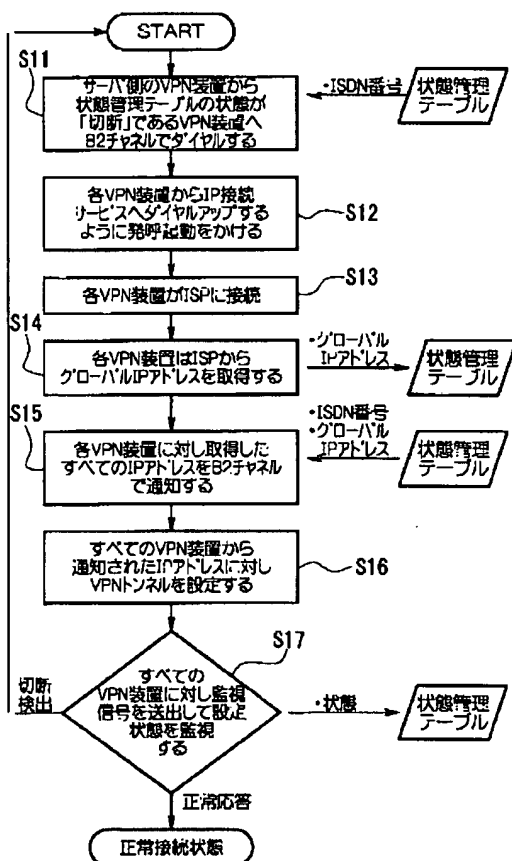
【図2】

VPN装置名	ISDN番号	グローバルIPアドレス	状態
A	06-4803-1111	X.X.X.X	接続
B	06-4804-2222	Y.Y.Y.Y	接続
C	06-4805-3333	Z.Z.Z.Z	接続
D	06-4806-4444	V.V.V.V	切断
E	06-4807-5555	W.W.W.W	切断

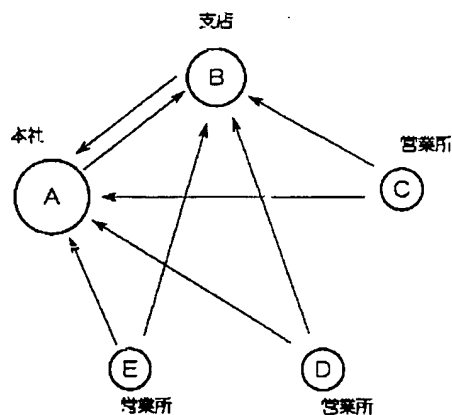
【图4】

WIN装置名	ISDN番号	グローバルIPアドレス	状態	スケジュール
A	06-4803-1111	X.X.X.X	接続	フル稼働
B	06-4804-2222	Y.Y.Y.Y	接続	日曜日の停止
C	06-4805-3333	Z.Z.Z.Z	接続	平日の日勤務のみ稼働
D	06-4806-4444	V.V.V.V	切断	平日の日勤務のみ稼働
E	06-4807-5555	W.W.W.W	切断	平日の日勤務のみ稼働

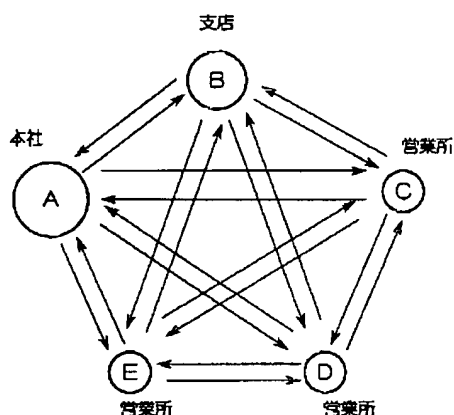
【図5】



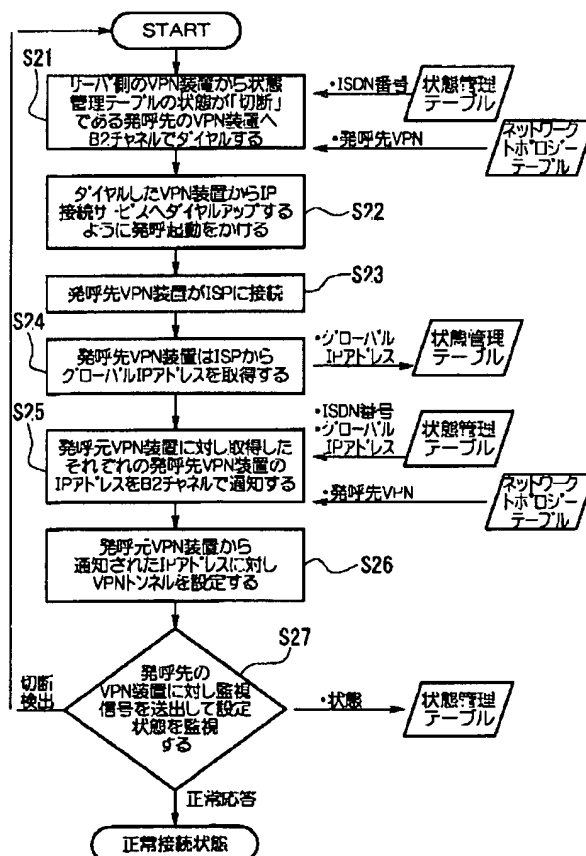
【図8】



【图6】



【图7】



フロントページの続き

(72)発明者 奥村 聡
大阪府大阪市中央区馬場町 3 番15号 西日
本電信電話株式会社内
(72)発明者 佐藤 勝彦
大阪府大阪市中央区馬場町 3 番15号 西日
本電信電話株式会社内

F ターム(参考) 5K024 AA61 CC09 CC10 GG01 GG03
GG05
5K030 GA00 HA08 HC01 HC05 HD09
KA05 KA14 MB01
5K101 KK02 KK16 LL03 LL05 MM07
PP03 QQ13 SS07 TT06 UU16